УДК 004.056
DOI: 10.26102/2310-6018/2023.43.4.029

Intelligent decision support system for assessing information security risks of ICS

A.D. Kirillova, A.M. Vulfin✉, V.I. Vasilyev, M.B. Guzairov

Ufa University of Science and Technology, Ufa, the Russian Federation

Abstract. The relevance of the article is due to the need to ensure information security of industrial control systems (ICS). Loss of control over industrial facilities can lead to undesirable consequences in a particular subject of the state or affect the economic indicators of the country as a whole as well as compromise the safety of the population. In this regard, this article aims to improve the procedure for quantitative assessment of information security risks as a necessary component of an integrated approach to ensuring information security, which helps to assess the feasibility of information security violation scenarios and identify their possible consequences for building an effective protection system. The architecture of a research prototype of an intelligent decision support system and a software implementation of tools for automating the modeling of attack scenarios and assessing the information security risks of ICS have been developed, the use of which makes it possible to increase the reliability and efficiency of information security risk assessment and, consequently, the choice of effective countermeasures at all stages of an industrial facility life cycle and its complex protection systems. The materials of the article are of practical value for information security specialists at all stages of the life cycle of distributed information and control systems of industrial facilities.

Keywords: information security risk assessment, intelligent decision support system, cognitive modeling, scenario modeling, graph models.

For citation: Kirillova A.D., Vulfin A.M., Vasilyev V.I., Guzairov M.B. Intelligent decision support system for assessing the risks of information security violations of ICS. *Modeling, Optimization and Information Technology*. 2023;11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1476 DOI: 10.26102/2310-6018/2023.43.4.029 (In Russ.).

Интеллектуальная система поддержки принятия решений при оценке рисков нарушения информационной безопасности АСУ ТП промышленных объектов

А.Д. Кириллова, А.М. Вульфин✉, В.И. Васильев, М.Б. Гузаиров

Уфимский университет науки и технологий, Уфа, Российская Федерация

Резюме. Актуальность статьи обусловлена необходимостью обеспечения информационной безопасности (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП) промышленных объектов. Потеря управления над промышленными объектами может привести к нежелательным последствиям в отдельном субъекте государства или отразиться на экономических показателях страны в целом, а также снизить безопасность жизнедеятельности населения. В связи с этим данная статья направлена на совершенствование процедуры количественной оценки рисков нарушения ИБ как необходимой составляющей комплексного подхода к обеспечению ИБ, позволяющей оценить реализуемость сценариев нарушения ИБ и выявить их возможные последствия для построения эффективной системы защиты. Разработана архитектура исследовательского прототипа интеллектуальной системы поддержки принятия решений и программная реализация инструментальных средств автоматизации моделирования сценариев атак и оценки рисков нарушения ИБ АСУ ТП промышленных объектов, применение которых позволяет повысить достоверность и оперативность оценки рисков нарушения ИБ и, следовательно, эффективность выбора контрмер на всех этапах жизненного цикла промышленного объекта и его комплексной системы защиты. Материалы статьи представляют практическую ценность для специалистов по ИБ на всех этапах жизненного цикла распределенных информационно-управляющих систем промышленных объектов.

Ключевые слова: оценка рисков нарушения информационной безопасности, интеллектуальная система поддержки принятия решений, когнитивное моделирование, сценарное моделирование, графовые модели.

Для цитирования: Кириллова А.Д., Вульфин А.М., Васильев В.И., Гузаиров М.Б. Интеллектуальная система поддержки принятия решений при оценке рисков нарушения информационной безопасности АСУ ТП промышленных объектов. *Моделирование, оптимизация и информационные технологии.* 2023;11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1476 DOI: 10.26102/2310-6018/2023.41.2.xxx (на англ.).

Introduction

The development of Industry 4.0 is based on the technologies of the Industrial Internet of Things (IIoT) and cyber-physical systems aimed at combining physical and digital production. Modern industrial automation systems are undergoing a digital transformation, which significantly aggravates the problem of ensuring information security of industrial control systems (ICS) of industrial facilities. The introduction of new technologies as well as the unification and close integration of production with the corporate information system and the external environment entails the emergence of many new vulnerabilities, threats and information security risks that were not previously typical for ICS.

Today, regulatory requirements aimed at improving the information security of ICS and critical information infrastructure (CII) objects have increased significantly. It is necessary to ensure partial or complete automation of the processing of large volumes of data on the state of ICS accumulated in modern information security systems, which will ultimately increase the efficiency of not only qualitative, but also quantitative assessment of information security risks and will improve the security of these objects under the influence of possible potential threats.

The problem of ensuring ICS information security is reflected in a number of Russian and international regulatory and methodological documents, as well as in the works of a number of Russian and foreign researchers.

The works [1-8] propose methods and technologies for assessing and analyzing information security risks based on the use of new methods, models and technologies for data mining. The greatest difficulty in this case is caused by the insufficient amount of available statistical information about threats and vulnerabilities, its inconsistency and incompleteness, which makes it difficult to form reliable assessments of information security risks and obtain final indicators of the level of ICS security.

Issues of modeling scenarios of computer attacks on ICS are reflected in research [9-11]. Analysis of the research showed that to build attack scenarios, tools have been developed that allow automating individual stages of this process. A comprehensive solution to the problem of modeling attack scenarios on ICS, based on the use of accumulated information from open international knowledge bases, has not been proposed.

The analysis of published papers generally shows that despite a significant amount of research in this subject area, the problem of adequate quantitative assessment of ICS information security risks and the selection of the appropriate composition of countermeasures needs further elaboration. With the increase in statistical data and the development of mathematical models of information security risk, threats and security incidents, the task of developing methods and algorithms for quantitative assessment of ICS information security risks, providing the ability to reliably assess the level of ICS security and its compliance with the requirements of regulatory documents, becomes relevant.

Therefore, the development of automation tools for modeling attack scenarios and assessing the information security risks of ICS is a relevant objective. It is proposed to include tools in the prototype of an intelligent decision support system (IDSS) at the stage of assessing the risks of information security of ICS.

Development of a functional model of the ICS information security risk assessment process

The proposed process for assessing the information security risks of ICS was developed as a result of an analysis of the existing regulatory and methodological support for information security of ICS[1,2,3,4] [12], as well as an analysis of current approaches to assessing information security risks. The evaluation process is formalized as a functional model in IDEF0 notation. The model of the process of quantitative assessment of information security risks of ICS is based on the construction of a hierarchy of fuzzy cognitive maps (FCM) for the zonal model of the protected object. The use of a hierarchy of models makes it possible to describe attack scenarios both within designated zones and for the entire industrial facility.

The essence of the applied cognitive modeling methodology [6-8, 13, 14] is the construction and subsequent analysis of FCM using the knowledge and experience of expert specialists in the subject area under consideration.

The decomposition of the first level of the functional model in Figure 1 displays the structure of the process of obtaining a quantitative assessment of the information security risks of the allocated ICS zones and the industrial system as a whole.

Based on the data collected by the inventory and accounting subsystems of information assets, as well as a detailed structural and functional description of the object, a set of models is constructed in accordance with the GOST 62443 series of standards, which makes it possible to decompose the task of assessing information security risks into a limited complexity set of elements for each of the selected zones.

Based on the recommendations of domestic and foreign regulatory documents and knowledge bases, information security specialists construct an attack graph, graph models of attack scenarios and models of attack patterns [14] using the tools proposed in the research. The hierarchy of graph models is an integral representation of information about possible chains of vulnerabilities, shortcomings in software implementation, and accumulated data about scenarios for implementing multi-step attacks by active groups of attackers. A feature of graph models is also the consideration of possible countermeasures (both organizational and technical) aimed at reducing the level of danger of the simulated attack scenarios.

[1] GOST R 56205-2014 IEC TS 62443-1-1 2009 Industrial communication networks. Security (cybersecurity) of the network and system. Part 1-1. Terminology, conceptual provisions and models. Moscow, Standartinform, 2014. (In Russ.).

[2] Methodology for assessing information security risks. FSTEC of Russia, 2021 URL: https://fstec.ru/component/attachments/download/2919 (accessed on 13.11.2023) (In Russ.)

[3] Requirements for ensuring the protection of information in automated control systems for production and technological processes at critical facilities, potentially hazardous facilities, as well as facilities that pose an increased danger to the life and health of people and the environment (approved by order of the FSTEC of Russia dated March 14, 2014 No. 31). Moscow, 2014. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (accessed on 13.11.2023). (In Russ.).

[4] Requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation (approved by order of the FSTEC of Russia dated December 25, 2017 No. 239). Moscow, 2017. URL: https://fstec.ru/component/attachments/download/1880 (accessed on 13.11.2023). (In Russ.).

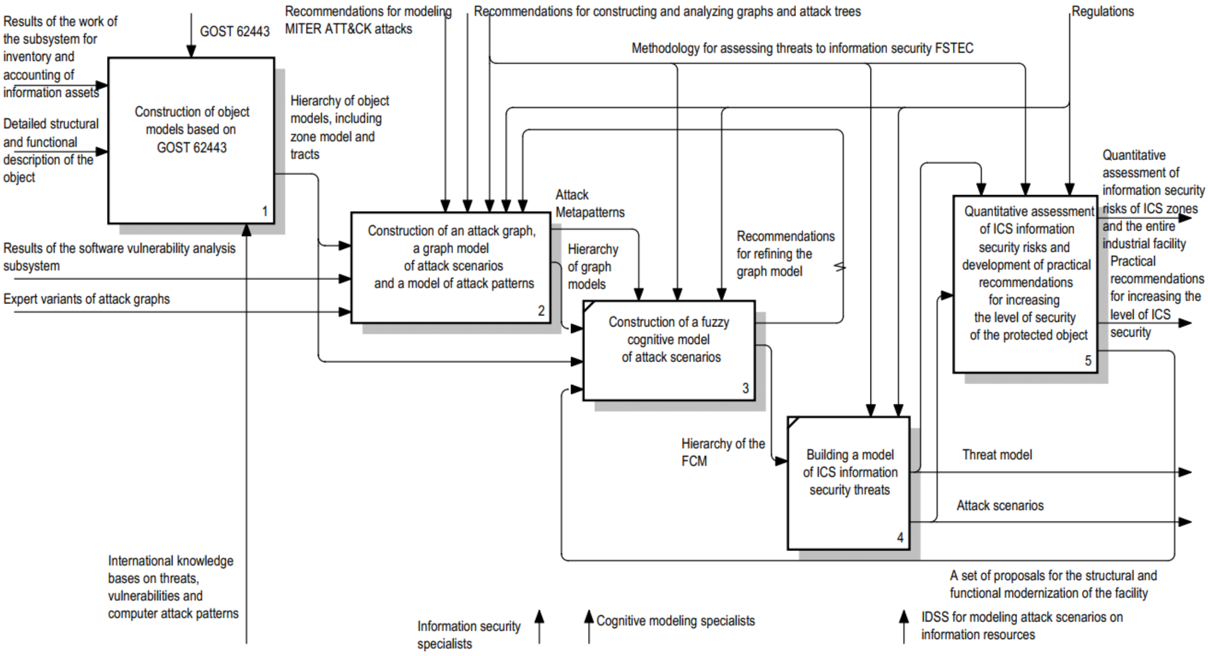
Results of the work of the subsystem for inventory and accounting of information assets
GOST 62443
Recommendations for modeling MITER ATT&CK attacks
Recommendations for constructing and analyzing graphs and attack trees
Regulations
Methodology for assessing threats to information security FSTEC
Detailed structural and functional description of the object
Construction of object models based on GOST 62443
1
Hierarchy of object models, including zone model and tracts
Results of the software vulnerability analysis subsystem
Expert variants of attack graphs
Construction of an attack graph, a graph model of attack scenarios and a model of attack patterns
2
Attack Metapatterns
Hierarchy of graph models
Recommendations for refining the graph model
Construction of a fuzzy cognitive model of attack scenarios
3
Hierarchy of the FCM
Building a model of ICS information security threats
4
Quantitative assessment of ICS information security risks and development of practical recommendations for increasing the level of security of the protected object
5
Quantitative assessment of information security risks of ICS zones and the entire industrial facility
Practical recommendations for increasing the level of ICS security
Threat model
Attack scenarios
A set of proposals for the structural and functional modernization of the facility
International knowledge bases on threats, vulnerabilities and computer attack patterns
Information security specialists
Cognitive modeling specialists
IDSS for modeling attack scenarios on information resources

Figure 1 – Decomposition diagram of the first level of the functional model of the ICS information security risk assessment process
Рисунок 1 – Диаграмма декомпозиции первого уровня функциональной модели процесса оценки рисков нарушения ИБ АСУ ТП промышленных объектов

At the stage of cognitive modeling of individual attack scenarios, cognitive modelers and information security specialists identify components (nodes, connections) of the graph model that require clarification, and also perform a convolution of scenarios in the form of nested FCM that describe the selected attack meta-patterns.

Based on the FCM hierarchy, fragments of the ICS information security model are constructed, which allows integrating, according to the FSTEC Methodology of Russia [13], information about the capabilities of the intruder, the consequences of attacks and current information security threats. Separate components of the threat model and developed attack scenarios are used to quantitatively assess information security risks for designated ICS zones. Based on the generated zonal assessments, a comprehensive information security risk assessment is constructed for the entire industrial facility. Based on information about attack scenarios that exploit existing or potential vulnerabilities and/or weaknesses in software, a list of countermeasures is generated and parameters for their deployment and operation are selected in order to increase the level of security of the facility as a whole. Based on several iterations of modeling, taking into account various attack scenarios, as well as lists of countermeasures and the distribution of their resources, practical recommendations are developed to improve the level of ICS security.

Development of a structural and functional organization of an IDSS for assessing ICS information security risks

The structural and functional organization of the developed IDSS in the tasks of assessing information security risks ICS (Figure 2) includes those proposed by the authors in [13-15]:

– hierarchical model of nested fuzzy grey cognitive maps (FGCM) for assessing the risks of information security of industrial facilities and an algorithm for its construction;

– method for quantitative assessment of ICS information security risks based on modeling attack scenarios using cognitive modeling technologies and machine learning methods;

– algorithms (constructing graph models and quantitative assessment of ICS information security risks based on modeling attack scenarios) and methods for quantitative assessment of ICS information security risks based on the construction of attack scenarios, characterized by the use of fuzzy cognitive modeling and machine learning methods to assess the level of security of selected ICS zones.

To reduce the time spent on assessing information security risks based on the basic principles of constructing open systems (functional decomposition, modularity, openness of interfaces for interaction with external systems), the following subsystems have been identified for collecting, processing and subsequent analysis of data:

– subsystem (SS_1) for processing and formalizing data on vulnerabilities, weaknesses and the composition of software and hardware of ICS (modules 2, 3);

– subsystem (SS_2) for constructing and analyzing a graph model of attack scenarios (modules 4, 5)

– subsystem (SS_3) of cognitive modeling and quantitative assessment of information security risks (modules 6, 7);

– subsystem (SS_4) for constructing fragments of the ICS information security threat model (modules 1, 8, 9).

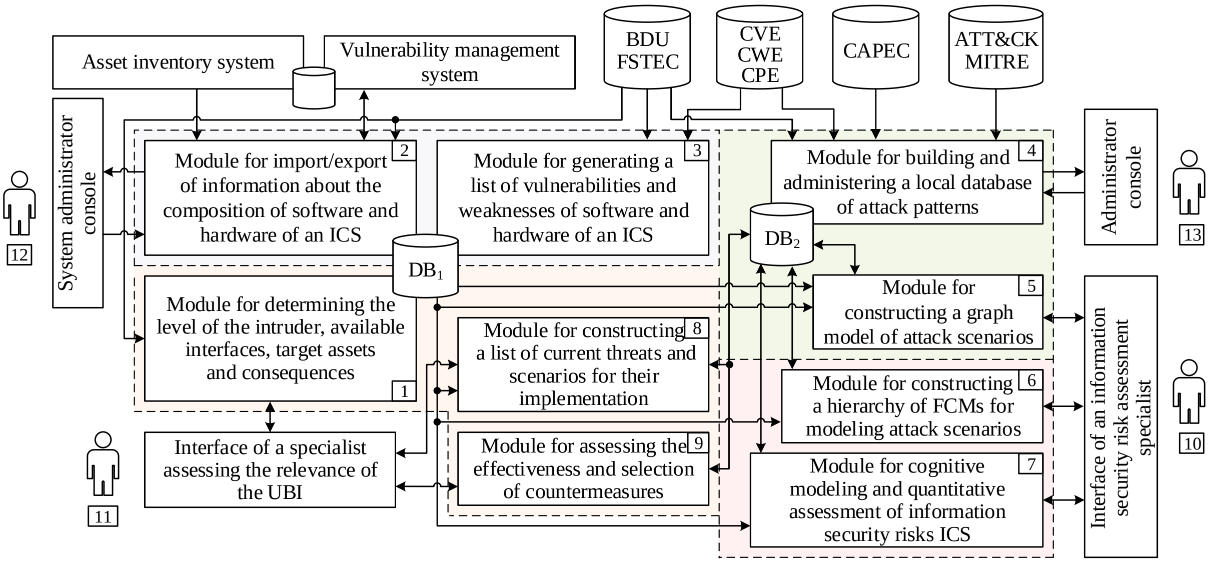
Asset inventory system
Vulnerability management system
BDU FSTEC
CVE CWE CPE
CAPEC
ATT&CK MITRE
System administrator console
Module for import/export of information about the composition of software and hardware of an ICS
2
Module for generating a list of vulnerabilities and weaknesses of software and hardware of an ICS
3
Module for building and administering a local database of attack patterns
4
Administrator console
13
12
DB₁
DB₂
Module for determining the level of the intruder, available interfaces, target assets and consequences
1
Module for constructing a list of current threats and scenarios for their implementation
8
Module for constructing a graph model of attack scenarios
5
Interface of an information security risk assessment specialist
Module for constructing a hierarchy of FCMs for modeling attack scenarios
6
10
Interface of a specialist assessing the relevance of the UBI
Module for assessing the effectiveness and selection of countermeasures
9
Module for cognitive modeling and quantitative assessment of information security risks ICS
7
11

Figure 2 – Structural and functional organization of an IDSS for assessing ICS information security risks

Рисунок 2 – Структурно-функциональная организация ИСППР в задачах оценки рисков нарушения ИБ АСУ ТП

Subsystem for processing and formalizing information about vulnerabilities, shortcomings and the composition of ICS software and hardware. Module (2) implements interaction with external inventory and vulnerability management systems, making it possible to automatically update information about the composition, configuration, physical and logical topology of the analyzed ICS in the local storage (relational DB_1). The module allows import and export of data on the composition of software and hardware. Administration of the process of importing data from external databases is under the control of the system administrator (12).

Based on accumulated data on the composition and organization of ICS and taking into account CPE identifiers and data from external storages NVD (CVE, CWE) and BDU FSTEC of Russia, module (3) helps to generate a list of vulnerabilities and weaknesses of the software and hardware of the analyzed system. Information from external databases is imported via API interfaces in established machine-readable formats (JSON and XML). The accumulated structured data is placed in DB_1 storage.

Subsystem for constructing and analyzing a graph model of attack scenarios. Module (5) provides the ability to construct a graph model of attack scenarios based on the formalization of the CPE-CVE-CWE-CAPEC chains and construct a graph of connections between the specified description identifiers in the graph DB_2 format based on Neo4j technologies and the Cypher language. The second graph model stored in DB_2 provides formalization of the connections CAPEC-ATT&CK (Techniques)-ATT&CK (Tactics)-Threats BDU FSTEC. Many connections between identifiers are built on the basis of cross-references in their descriptions and are supplemented by manual marking.

Module (4) provides the ability to import data from external storages, translate them into the DB_2 data schema and administer the process of processing accumulated data. The administrator (13) of subsystems for updating data from external sources ensures control of the interaction processes with external storages and the relevance of the stored data.

Subsystem of cognitive modeling and quantitative assessment of information security risks. Module (6) for constructing a hierarchy of FCM helps to simulate attack scenarios based on collapsing a graph model generated based on queries to DB_2 for the current set of identified vulnerabilities with an assessment of their level of danger. Module (7) is designed to obtain a quantitative assessment of information security risks for selected zones of an industrial facility based on the results of cognitive modeling. A specialist (10) in assessing and modeling information security risks performs operations to prepare and transform the graph model into a decomposition of the cognitive map corresponding concepts of the current level of analysis.

Subsystem for constructing fragments of the ICS information security threat model. Module (1) is intended to formalize information about the level of the intruder, available interfaces, target assets and possible consequences of the implementation of threats. A specialist (11) in assessing current threats using developed tools and based on the FSTEC Methodology determines the main parameters necessary for the formation of quantitative assessments of information security risks. Next, they carry out actions to clarify, adjust and analyze the previously obtained attack scenarios. Module (8) based on a graph model helps to generate implementation scenarios for current threats. Module (9) makes it possible to obtain direct quantitative assessments of information security risks for selected ICS zones and generate a list of countermeasures with the ability to quantitatively assess the effectiveness of their application both for individual zones and for the entire ICS as a whole (based on assessments of information security risks and costs for their implementation).

Development of an architecture and a set of object-oriented IDSS models for assessing ICS information security risks

According to ISO/IEC/IEEE 42010 and SEI (Software Engineering Institute) guidelines, system architecture is “the fundamental concepts and properties of a system in its environment, embodied in its elements, relationships, and principles of its design and evolution”.

Models (informational, functional, behavioral) obtained as a result of analyzing the requirements for an IDSS are the initial data for the stage of detailed design of an IDSS architecture. At the end of the design stage, models of data, architecture and subsystems should be formed.

To carry out requirement analysis and further design an IDSS, use case diagrams (UCDs) have been developed in UML notation, demonstrating how users with established roles can interact with the system.

Dedicated user roles: specialist in assessing current threats; system administrator; administrator of the data update subsystem from external sources.

UCD$_1$ reveals the process of filling local DB$_1$ based on the results of inventory and importing data from external sources when users interact with SS$_1$ (Figure 3 where 11 is a specialist in assessing current threats; 12 is a system administrator; 13 is an administrator of the data update subsystem from external sources).

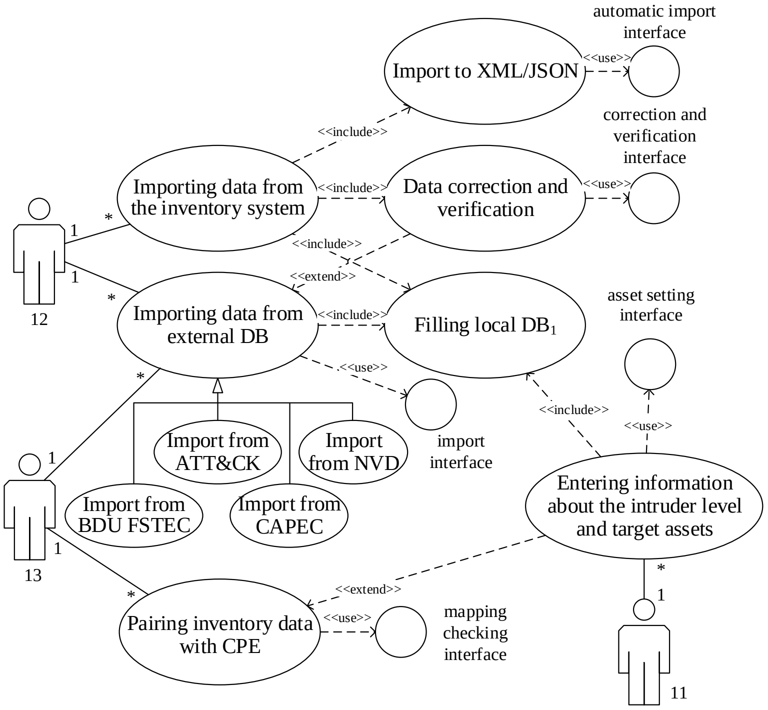
automatic import interface
Import to XML/JSON
<<use>>
<<include>>
correction and verification interface
Importing data from the inventory system
<<include>>
Data correction and verification
<<use>>
1
*
<<include>>
<<extend>>
1
*
Importing data from external DB
<<include>>
Filling local DB1
asset setting interface
12
<<use>>
*
<<include>>
<<use>>
Import from ATT&CK
Import from NVD
import interface
1
Entering information about the intruder level and target assets
Import from BDU FSTEC
Import from CAPEC
1
13
*
<<extend>>
1
*
Pairing inventory data with CPE
<<use>>
mapping checking interface
11

Figure 3 – UCD$_1$ filling local DB$_1$ based on inventory results and importing data from external sources when users interact with SS$_1$

Рисунок 3 – ДВИ$_1$ наполнения локальной БД$_1$ по результатам инвентаризации и импорт данных из внешних источников при взаимодействии пользователей с ПС$_1$

UCD$_1$ includes basic precedents for importing data from systems external to the projected IDSS with the required level of decomposition. For each of the actors, typical interfaces are given, through which the use case is implemented.

UCD$_2$ (Figure 4) reveals the process of user interaction with SS$_2$ when constructing and using a graph model of attack scenarios.

Detailing of UCD$_2$ precedents demonstrates the main stages of interaction with external databases and knowledge (NVD, MITRE ATT&CK and BDU FSTEC) during the construction of a graph model of attack scenarios based on cross-relationships between entities describing both a set of software and hardware vulnerabilities and tactics and techniques used by attackers.

UCD$_3$ (Figure 5, where 10 is specialist in assessing and modeling information security risks) reveals the process of quantitative assessment of the information security risks of an industrial facility and assessing the effectiveness of the choice of countermeasures when interacting with users with SS$_3$ and SS$_4$.

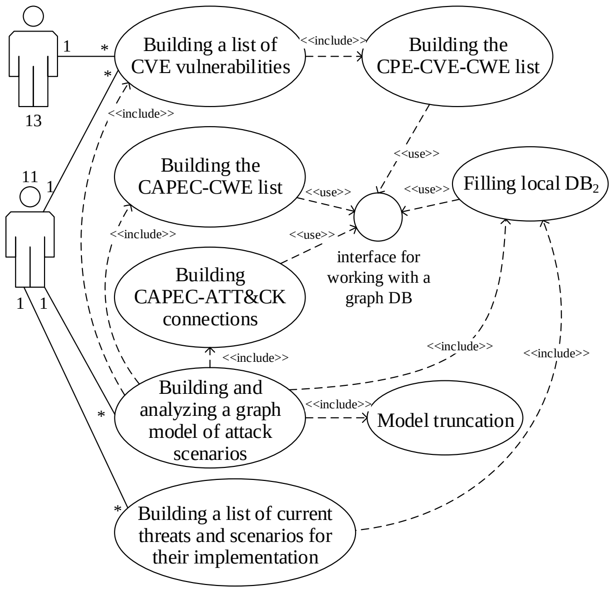
13
11
Building a list of CVE vulnerabilities
Building the CPE-CVE-CWE list
Building the CAPEC-CWE list
Filling local DB$_2$
interface for working with a graph DB
Building CAPEC-ATT&CK connections
Building and analyzing a graph model of attack scenarios
Model truncation
Building a list of current threats and scenarios for their implementation
<<include>>
<<use>>
1
*

Figure 4 – UCD$_2$ user interaction with SS$_2$ when constructing and using a graph model of attack scenarios

Рисунок 4 – ДВИ$_2$ взаимодействия пользователей с ПС$_2$ при построении и использовании графовой модели сценариев атак

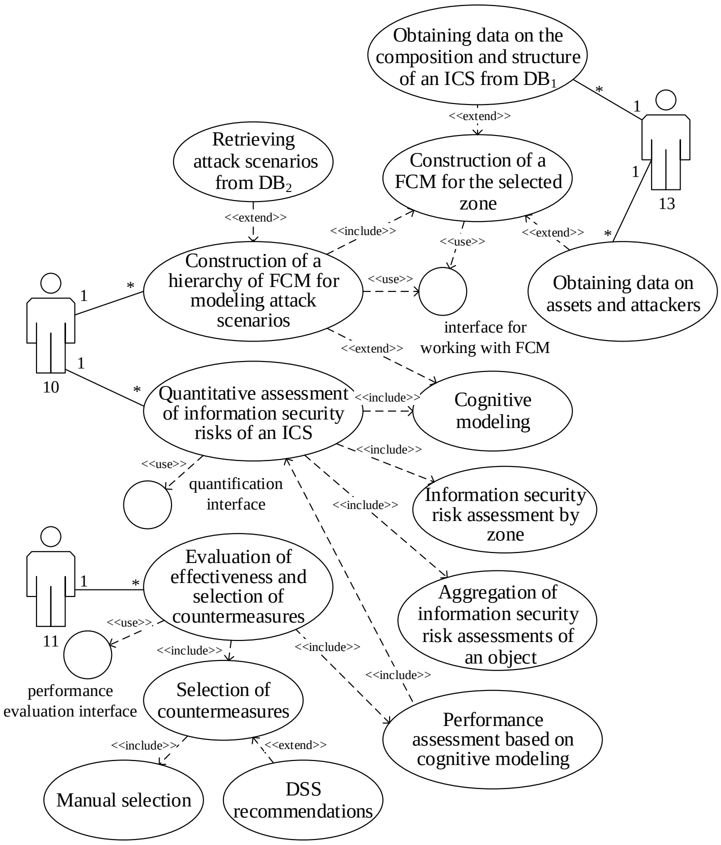
Obtaining data on the composition and structure of an ICS from DB$_1$
13
10
11
Retrieving attack scenarios from DB$_2$
Construction of a FCM for the selected zone
Construction of a hierarchy of FCM for modeling attack scenarios
interface for working with FCM
Obtaining data on assets and attackers
Quantitative assessment of information security risks of an ICS
Cognitive modeling
quantification interface
Information security risk assessment by zone
Aggregation of information security risk assessments of an object
Evaluation of effectiveness and selection of countermeasures
performance evaluation interface
Selection of countermeasures
Performance assessment based on cognitive modeling
Manual selection
DSS recommendations
<<include>>
<<extend>>
<<use>>
1
*

Figure 5 – UCD$_3$ for quantitative assessment of information security risks of an industrial facility during user interaction with SS$_3$ and SS$_4$

Рисунок 5 – ДВИ$_3$ количественной оценки рисков нарушения ИБ промышленного объекта при взаимодействии пользователей с ПС$_3$ и ПС$_4$

The developed UCDs for dedicated user roles are the basis for further specification of functional requirements. The specification of functional and non-functional requirements is the basis for the subsequent detailed design of the IDSS architecture.

One of the key stages in the detailed design of the IDSS architecture is a class diagram, which demonstrates an object-oriented decomposition of key subsystems. Figure 6 shows a fragment of the SS_3 class diagram in UML notation.

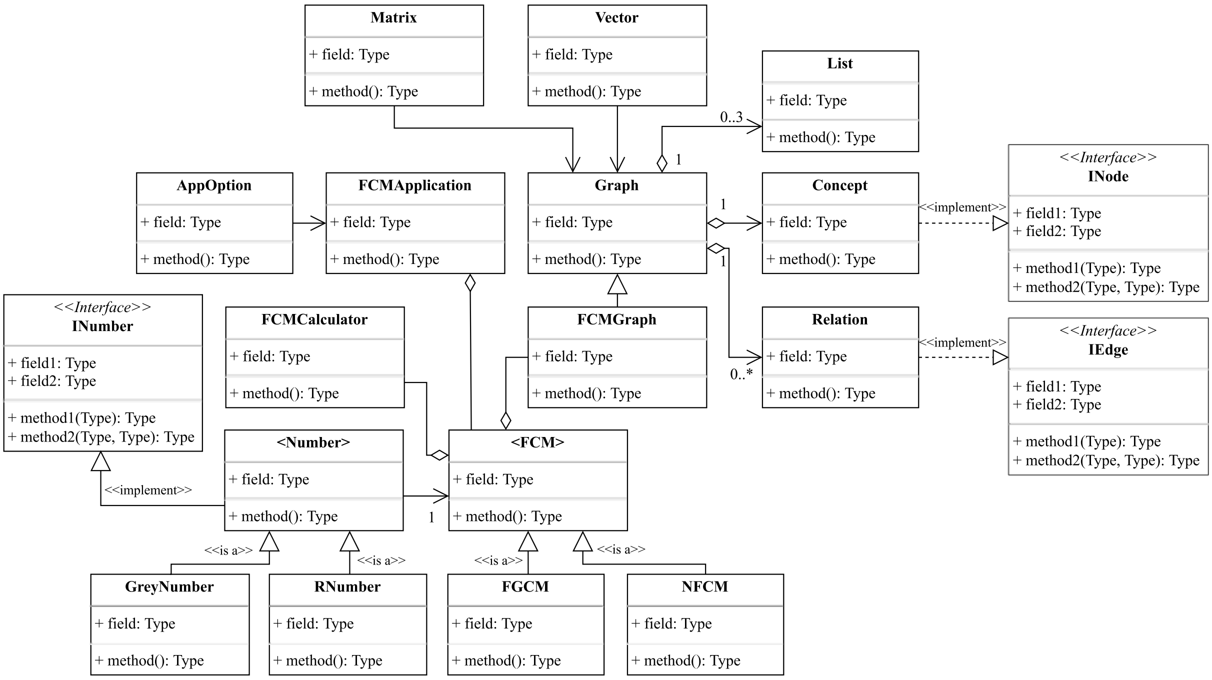

Figure 6 – Fragment of the SS_3 class diagram in UML notation
Рисунок 6 – Фрагмент диаграммы классов $ПС_3$ в нотации UML

A fragment of the SS_3 class diagram demonstrates the static structural hierarchy of key entities implemented in the process of object-oriented analysis and design in the form of a set of classes, interfaces and their interactions.

A fragment of the logical data model DB_1 is presented, which describes the structure and relationship of the main entities of the subject area used to create a data warehouse about threats, vulnerabilities and scenarios for their implementation SS_1 and SS_4 based on interaction with external knowledge bases BDU FSTEC, NVD and MITRE (Figure 7).

The DB_2 information model includes two sets of entities connected by relationships. This allows to use the Cypher query language to analyze the hierarchy of entities. Including, for analysis taking into account indirect connections in the form of an oriented weighted graph. The use of a specialized graph DBMS helps to:

– simplify the analysis of graph structures in the process of transition between adjacent vertices of a directed graph in one step, excluding the recursive pass and the join operation for each level of data analysis in relational DB;

– provide a data visualization interface.

ATT&CK for ICS helps to create a more complete knowledge base when assessing the relevance and implementation of protective measures. Using ATT&CK provides insight into potential threats and attacker actions. Information security specialists can make decisions by matching the attacker's actions and behavior with specific countermeasures that can be deployed in the ICS environment (Figure 8).

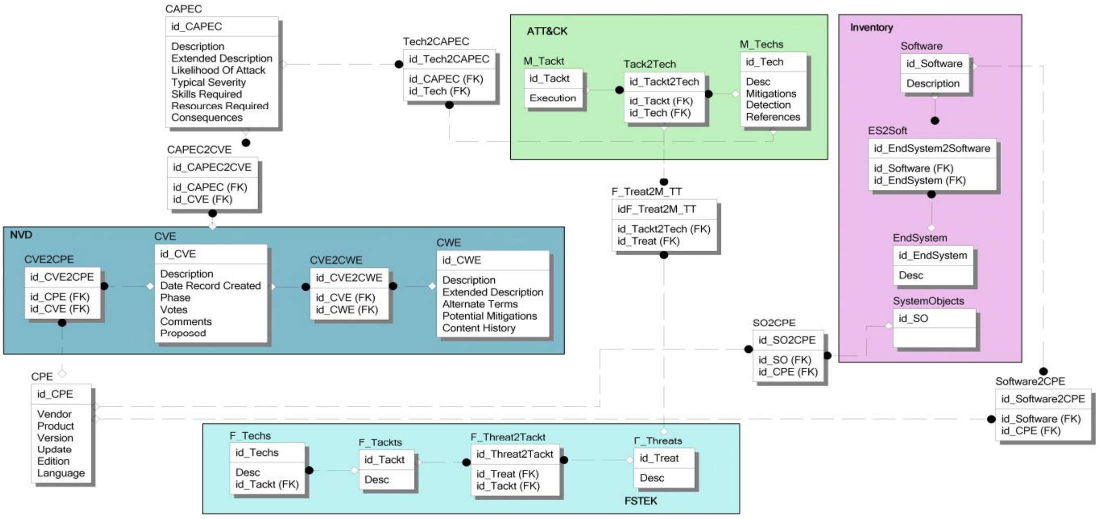

Figure 7 – Fragment of the logical data model of DB_1 for SS_1 and SS_4
Рисунок 7 – Фрагмент логической модели данных $БД_1$ для $ПС_1$ и $ПС_4$

Source data were imported from external ATT&CK storage (Enterprise, Mobile and ICS) as JSON files in STIX 2.1 (Structured Threat Information Expression) format to describe CTI (Cyber Threat Intelligence).

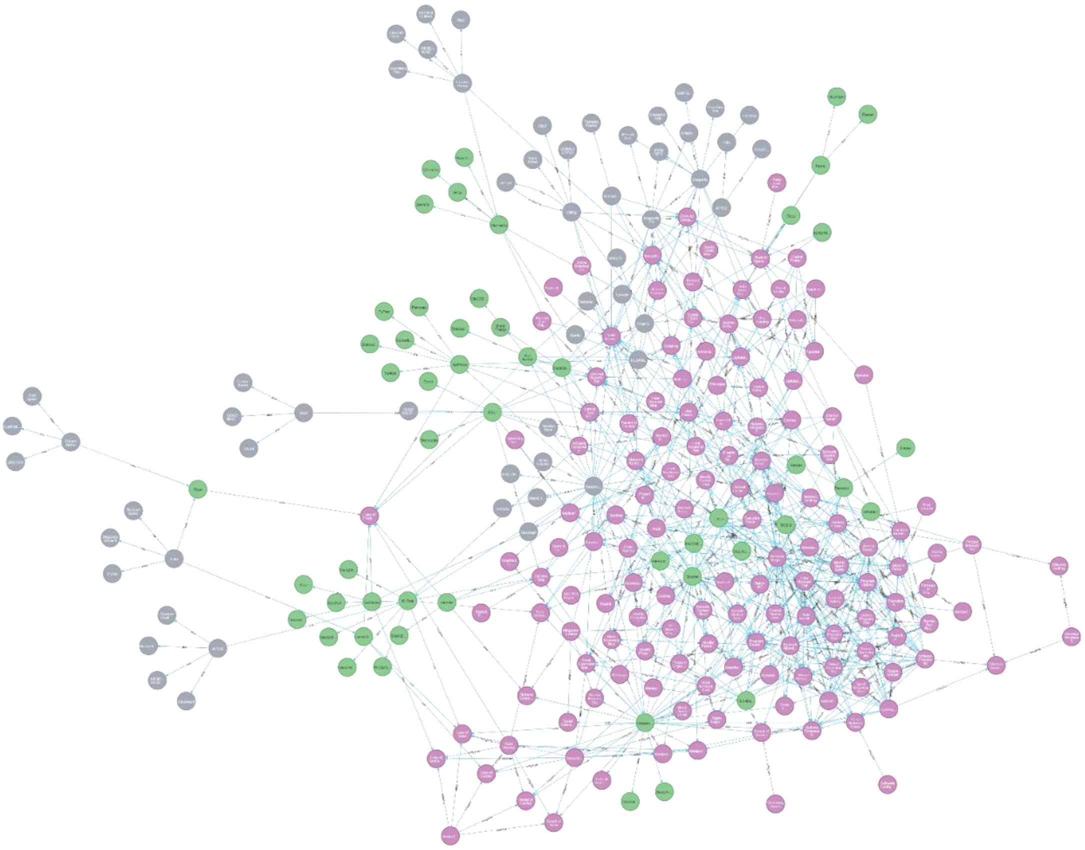

Figure 8 – Fragment of a graph describing the connections between entities, tactics, techniques and software used by attackers to carry out an offence
Рисунок 8 – Часть графовой модели, характеризующей связи между объектами, тактиками, техниками и программным обеспечением, используемым нарушителями при реализации атаки

The first set of entities (Table 1, Figure 9) is built on the MITRE ATT&CK for ICS knowledge base on attacker behavior in the ICS technology domain, reflecting the various stages of the attack lifecycle, as well as the system components it targets[5,6]. The structure of the initial stages of attacks affecting the IT infrastructure through tactics, techniques and procedures, as well as the actions that attackers take against the systems and functions of ICS, is revealed.

Table 1 – Description of the entities of the logical model of the graph DB$_2$ "Threats"
Таблица 1 – Описание сущностей логической модели графовой БД2 «Угрозы»

No	Entity	Description	Key entity characteristics
1	ICS Techniques ICS Subtechniques	Techniques represent "how" an attacker achieves a tactical goal by performing an action	ID, Sub-techniques, Tactic, Platforms, CAPEC ID, Contributors, Version, Created, Last Modified
2	ICS Tactics	Tactics are the detailing of an ATT&CK technique or subtechnique. This is the attacker's tactical goal: the reason for the action	ID, Created, Last Modified
3	ICS Mitigations	Mitigations represent security concepts and classes of technology that can be used to prevent the successful execution of a technique	ID, Version, Created, Last Modified
4	ICS Data Sources	Data sources represent the various topics/topics of information that can be collected by sensors/logs. Data sources also include data components that identify specific properties/values of the data source relevant to the detection of ATT&CK techniques	ID, Platforms, Collection Layers, Contributors, Version, Created, Last Modified
5	ICS Groups	Clusters of activities that are tracked by a common name in the security community (name aliases possible)	ID, Contributors Version, Created, Last Modified
6	ICS Software	Custom or commercial code, operating system utilities, open source software, or other tools used for behavior modeled in ATT&CK (name aliases possible)	ID, Type, Platforms, Version, Created, Last Modified

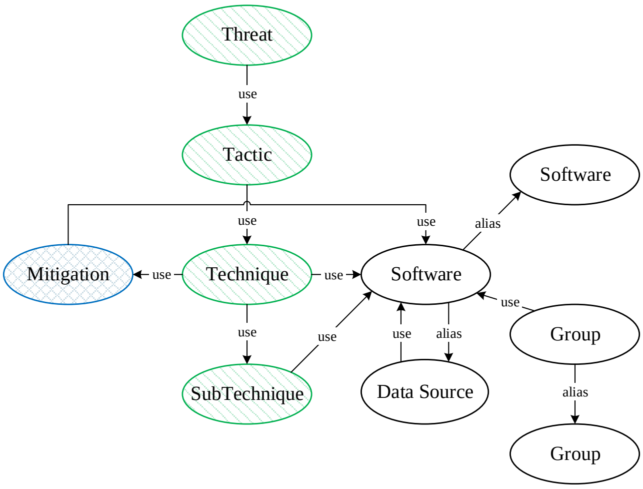

Figure 9 – Fragment of the logical data model of graph DB$_2$ "Threats"
Рисунок 9 – Фрагмент логической модели данных графовой БД2 «Угрозы»

[5] Import Mitre Att&ck into Neo4j database. URL: https://github.com/vmapps/attack2neo (accessed on 13.11.2023).
[6] STIX data representing MITRE ATT&CK. URL: https://github.com/mitre-attack/attack-stix-data (accessed on 13.11.2023).

The second set of entities (Table 2, Figure 10) of the graph DB$_2$ is built on the basis of GraphKer and the NVD and MITRE ATT&CK knowledge bases for ICS and describes “Scenarios” of attacks[7].

Table 2 – Description of the entities of the logical model of the graph DB$_2$ “Scenarios” (fragment)
Таблица 2 – Описание сущностей логической модели графовой БД$_2$ «Сценарии» (фрагмент)

No	Entity	Description	Key entity characteristics
1	CPE	Template for describing the platform containing the vulnerability	ID
2	CVE	Description of the vulnerability from the NVD database	ID
3	CWE	Description of the class of vulnerabilities – “weaknesses” in the implementation of software and hardware from the NVD database	Functional_Areas, Description, Affected_Resources, Submission_Name, Name
4	CAPEC	Description of the CAPEC pattern	Submission_Name, Description, Name, Skills_Required, Mitigations, Resources_Required, Likelihood_Of_Attack, Typical_Severity

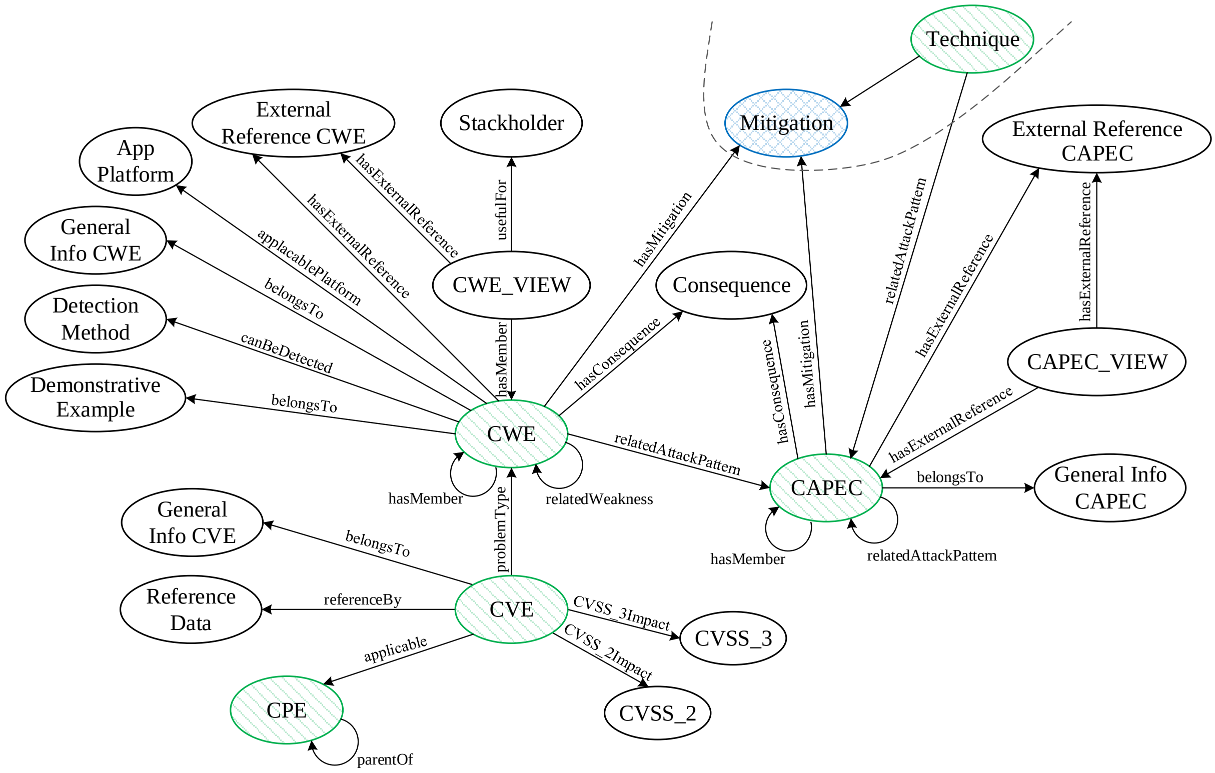

Figure 10 – Fragment of the logical data model of DB$_2$ “Scenarios”
Рисунок 10 – Фрагмент логической модели данных БД$_2$ «Сценарии»

Key relationships between selected entities help to display a variety of types of relationships and flexibly customize search scenarios using the Cypher query language.

[7] Open Source Tool - Cybersecurity Graph Database in Neo4j. GraphKer. URL: https://github.com/amberzovitis/GraphKer (accessed on 13.11.2023).

The development of the system is based on extensive use of existing architectural patterns. Figure 11 shows a fragment of the SS_3-SS_4 component diagram in UML notation with the implementation of the Model-View-Controller (MVC) pattern.

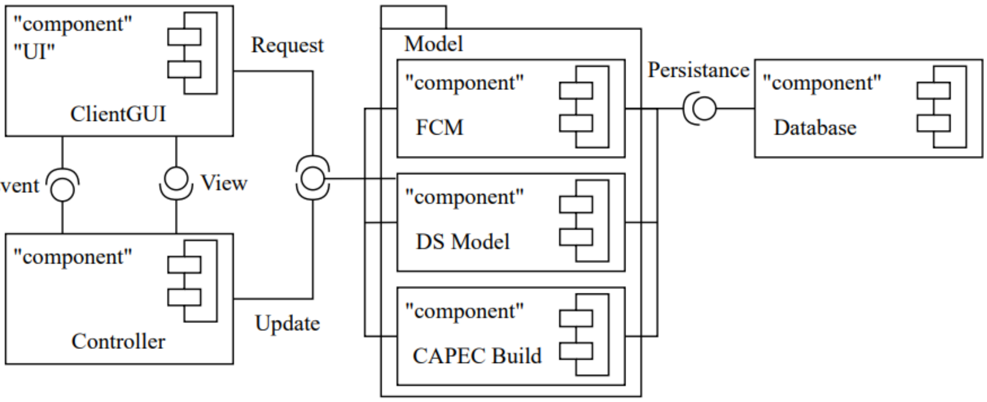

Figure 11 – Diagrams of SS_3-SS_4 components in UML notation with the implementation of the Model-View-Controller pattern
Рисунок 11 – Диаграммы компонентов $ПС_3$-$ПС_4$ в нотации UML с реализацией паттерна «модель-представление-контроллер»

As part of the software architecture, the main logical components SS_3-SS_4 are highlighted (Table 3):

1. The model that manages system data and operations on it.
2. The presentation component helps to display data for the user.
3. The controller component interacts with the user, initiates operations in the model and controls the operation of the presentation component.

Table 3 – Description of packages and modules of SS_3-SS_4 component diagrams
Таблица 3 – Описание пакетов и модулей диаграммы компонентов $ПС_3$-$ПС_4$

No	Component/module name	Description
1	UI	A component that provides visualization and maintenance of the GUI event queue (representation implementation) of the client for creating and editing FCM
2	Controller	Component that performs operations in the model (controller)
3	Model	A component containing models for managing system data and operations on them
4	FCM	Component (part of the Model component) of the software implementation of FCM
5	DS Model	Component (part of the Model component) of the software implementation of FCM learning algorithms for optimizing weight coefficients using genetic (evolutionary) algorithms
6	CAPEC Build	A component (part of the Model component) of a software implementation of a hierarchical representation of chains of events based on a graph model
7	Database	Local database for storing the current state of the application instance (ensuring persistence)

Thus, object-oriented analysis and design of subsystems as part of the IDSS were performed.

Application of an IDSS in assessing the risks of information security of ICS

In paper [15], the authors, based on the stages of analysis and modeling of a protected object presented in the GOST 62443 series of standards, built a set of models of an ICS consisting of a basic, object and zonal model using the example of a fragment of a geographically distributed system – ICS of the oil delivery point in a main pipeline system designed to automate the control and operational control of the technological process, including the collection of data on the technological parameters of the process: flow, level, temperature, pressure, density and humidity of the pumped oil.

For detailed modeling of attack scenarios, a set of developed tools was used as part of the IDSS.

Figure 12 shows a fragment of the scenario level, revealing the "vulnerability-weakness-pattern" chain for one selected vulnerability "CVE-2019-6812" generated using a query in the Cypher language:

```
MATCH (cve:CVE)-[:Problem_Type]-(cwe:CWE)-[:RelatedAttackPattern]-(capec:CAPEC)
MATCH (cve:CVE)-[:Problem_Type]-(cwe:CWE)-[:hasMitigation]-(mitigation:Mitigation)
WHERE (cve.Name starts with ("CVE-2019-6812"))
RETURN  cve, cwe, capec, mitigation
```

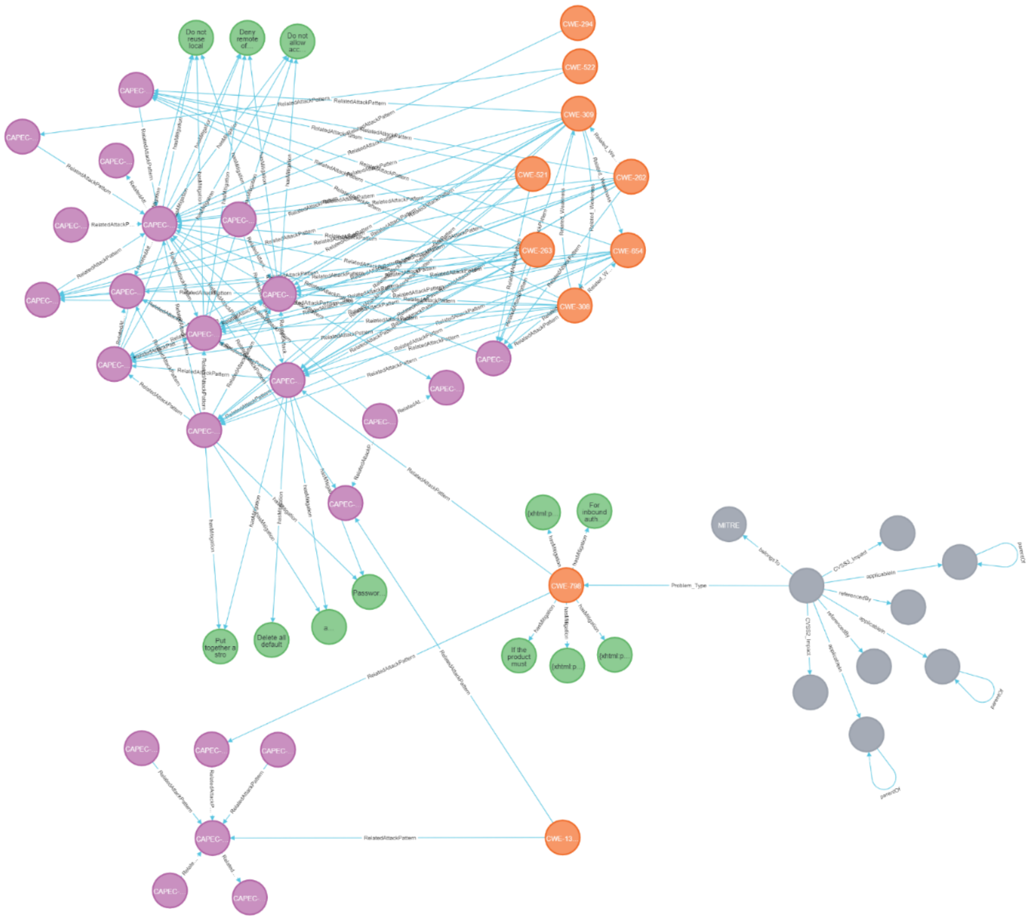

Figure 12 – Fragment of the scenario level demonstrating the "vulnerability-weakness-pattern" chain for one selected vulnerability "CVE-2019-6812"
Рисунок 12 – Фрагмент сценарного уровня, раскрывающий цепочку «уязвимость-слабость-шаблон» для одной выбранной уязвимости «CVE-2019-6812»

Next, the remaining stages of the information security risk assessment process were completed (Figure 1).

The following formal formulation of the multicriteria optimization problem (1) has been carried out, taking into account the possibility of minimizing the information security risk assessment for a selected area of an industrial facility and assessing the effectiveness of using countermeasures in various modeling scenarios with different options for specifying the objective function:

$$\text{а) } X_R \to min, \qquad \text{б) } \sum X_R \to min\,, \qquad \text{в) } \Phi\left(W_{C_C^i,C_S^j}\right) \to min, \qquad (1)$$

where $\Phi(\cdot)$ is a criterion for the effectiveness of using countermeasures; X_R is the information security risk assessment (the steady-state value of the state variable of the FCM concept, characterizing the assessment of information security risk – C_R). The weights of the FCM $W_{C_C^i,C_S^i}$ are considered as optimized parameters, characterizing the distribution of allocated resources for the implementation of countermeasures C_C^i in order to reduce the likelihood of an attack scenario C_S^j. To optimize the weight coefficients of the FCM, a genetic algorithm (GA) was used to ensure that the optimal solution to the problem was found.

To assess information security risks, the following modeling scenarios are considered:

Scenario A. A standard set of countermeasures was used.

Scenario B. Countermeasures are selected based on the IDSS recommendations of the scenario level of modeling.

Scenario C. Countermeasures are selected based on the IDSS recommendations at the scenario level of modeling with optimization of countermeasure resources using a GA.

Table 4 presents the results of computational experiments to assess the information security risk of the ICS for various attack scenarios. Using a GA, a set of weighting coefficients of a FCM was obtained, characterizing the optimal distribution of costs for implementing the necessary countermeasures to reduce the information security risk. The magnitude of the information security risk here was assessed in relative units in relation to the cost of the target information resources of the ICS; the effectiveness of the countermeasures was assessed by the criterion of reducing the achieved level of information security risk.

Table 4 – Results of the information security risk assessment of the ICS of the oil delivery point
Таблица 4 – Результаты оценки рисков нарушения ИБ АСУ ТП ПСП с оптимизацией весов НКК

Characteristics of target concepts	Risk assessment in the range of grey numbers		
	Scenario A	Scenario B	Scenario C
Information security risk assessment for the facility as a whole	[0.18; 0.26]	[0.09; 0.14]	[0.038; 0.070]
Assessing the effectiveness of countermeasures	[-; -]	[0.15; 0.20]	[0.218; 0.249]

The final state diagram of the target concepts of the FCM characterizing the assessment is shown in Figure 13, where X_{11} is a violation of the normal operating mode of the ICS; X_{12} is the failure of the company to fulfill contractual obligations; X_8 is the cost estimation of countermeasures; X_{15} is assessing the countermeasure effectiveness; X_{16} is the final information security risk assessment; along the ordinate is the value range of grey estimates of the state of concepts.

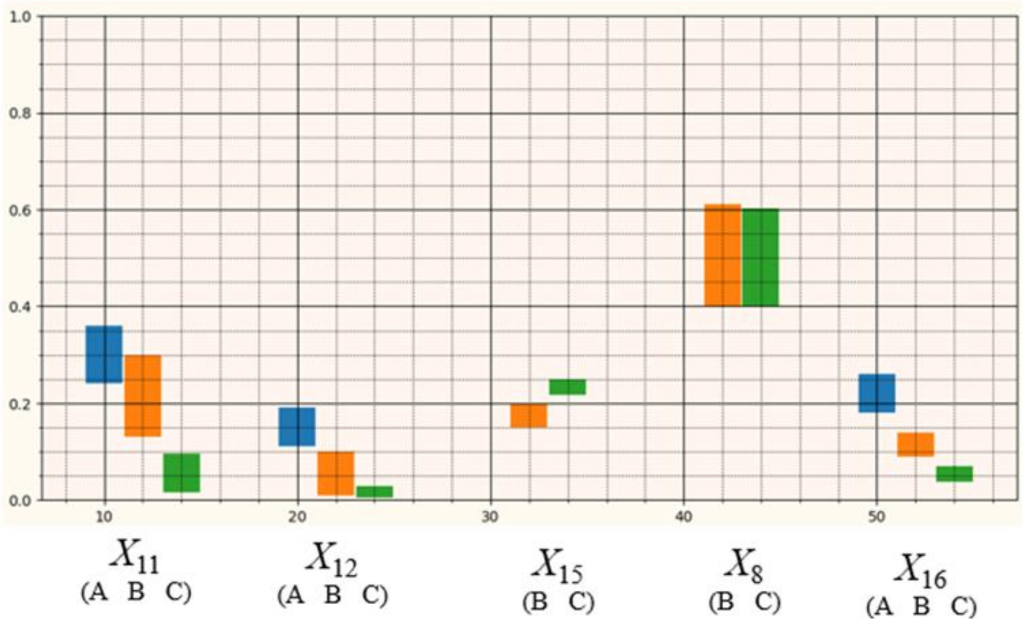

Figure 13 – State of target concepts of the FCM (along the ordinate is the value range of grey estimates of the state of concepts)
Рисунок 13 – Состояние целевых концептов НКК (по оси ординат – диапазон значения серых оценок состояния концептов)

Discussion

The use of software implementation of the developed method, models and algorithms for assessing the information security risks of ICS made it possible, after optimizing the distribution of resources allocated for countermeasures, to reduce the spread of expert assessments by 70–80 %, as well as increase the security of a specific ICS, reduce the preliminary estimate of the cost of operating the proposed protective measures. The duration of the procedure for modeling attack scenarios and assessing information security risks has decreased by 2.5 times.

Conclusion

The architecture of an intelligent decision support system has been developed, including software implementation of tools for automating information security risk assessment and modeling attack scenarios. The proposed system helps to collect information about the weak points of the ICS infrastructure, the most dangerous vulnerabilities and potential weaknesses of the system’s software and hardware, identify the potentially most successful attack scenarios, and assess their consequences for an industrial facility.

The conducted computational experiments showed that at the stages of designing and implementing countermeasures, the time spent on modeling attack scenarios was reduced by more than 2.5 times; the efficiency of operating countermeasures increased by 15 % by optimizing the distribution of resources for their use; the quantitative assessment of the level of information security risk for the protected object as a whole decreased by 10 %; the proposed solutions make it possible to generate an extended list of countermeasures based on the knowledge bases of BDU FSTEC, ATT&CK, NVD for each of the designated security zones.

The practical significance of the research results lies in the possibility of solving with their help applied problems of assessing the risks of information security of ICS, increasing the validity of the obtained quantitative assessments of information security risks with consideration to the impact of uncertainty factors.

REFERENCES

1. Papageorgiou E.I. Fuzzy cognitive maps for applied sciences and engineering: from foundations to extensions and learning algorithms. *Intelligent Systems Reference Library 54, Springer Science & Business Media*. 2013;54:411.
2. Salmeron J.L. et al. Learning fuzzy cognitive maps with modified asexual reproduction optimisation algorithm. *Knowledge-Based Systems*. 2019;163:723–735.
3. Novokhrestov A.K., Nikiforov D.S., Konev A.A., Shelupanov A.A. Model of threats to automatic system for commercial accounting of power consumption. *Proceedings of TUSUR University*. 2016;19(3):111–114. (In Russ.).
4. Guzairov M.B., Mashkina I.V. *Information security management based on intelligent technologies.* Moscow, Mechanical Engineering. 2013; 241 p. (In Russ.).
5. Efimov B.I., Lozhnikov P.S. Analysis of the impact of threats to change and block responses of experts in online survey systems. *Journal of Physics: Conference Series. IOP Publishing.* 2020;1546(1):012079.
6. Vasilyev V.I., Vulfin A.M., Guzairov M.B. Evaluation of Information Security Risks with Use of Rule-Based Fuzzy Cognitive Maps. *Information Security*. 2018;24(4):266–273. (In Russ.).
7. Vasilyev V.I., Vulfin A.M., Guzairov M.B., Kartak V.M., Chernjahovskaja L.R. Cybersecurity risk assessment of industrial objects' ACS of TP on the basis of nested fuzzy cognitive maps technology. *Informacionnye tehnologii.* 2020;26(4):213–221. (In Russ.).
8. Vasilyev V.I., Vulfin A.M., Kudryavtseva R.T. Analysis and management of information security risks using cognitive modeling technology. *Proceedings of TUSUR University*. 2017;20(4):61–66. (In Russ.).
9. Noel S., Harley E., Tam K.H., Limiero M., Share M. CyGraph: graph-based analytics and visualization for cybersecurity. *Handbook of Statistics. Elsevier*. 2016;35:117–167.
10. Yeboah-Ofori A. Cyber security threat modeling for supply chain organizational environments. *Future internet*. 2019;11(3):63.
11. Zografopoulos I., Ospina J., Liu X., Konstantinou C. Cyberphysical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access.* 2021;9:29775–29818.
12. Vasilyev V.I., Kirillova A.D., Kukharev S.N. Cybersecurity of APCS: modern trends and approaches (current state, perspectives). *Vestnik UrFO. Security in the Information Sphere.* 2018;30(4):66–74. (In Russ.)
13. Vasilyev V.I., Vulfin A.M., Guzairov M.B., Kirillova A.D. Interval Estimation of Information Risks with use of Fuzzy Grey Cognitive Maps. *Informacionnye tehnologii.* 2018;24(10):657–664. (In Russ.)
14. Vasilyev V.I., Kirillova A.D., Vulfin A.M. Cognitive modeling of the cyber attack vector based on CAPEC methods. *Voprosy kiberbezopasnosti*. 2021;42(2):2–16. (In Russ.)
15. Vasilyev V.I., Vulfin A.M., Kirillova A.D. Analysis and management of ICS cybersecurity risks based on cognitive modeling. *Modeling, Optimization and Information Technology*. 2022;10(2). URL: https://moitvivt.ru/ru/journal/pdf?id=1184 DOI: 10.26102/2310-6018/2022.37.2.022 (In Russ.).

СПИСОК ИСТОЧНИКОВ

1. Papageorgiou E.I. Fuzzy cognitive maps for applied sciences and engineering: from foundations to extensions and learning algorithms. *Intelligent Systems Reference Library 54, Springer Science & Business Media*. 2013;54:411.
2. Salmeron J.L. et al. Learning fuzzy cognitive maps with modified asexual reproduction optimisation algorithm. *Knowledge-Based Systems*. 2019;163:723–735.

3. Новохрестов А.К., Никифоров Д.С., Конев А.А., Шелупанов А.А. Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов. *Доклады ТУСУР*. 2016;19(3):111–114.
4. Гузаиров М.Б., Машкина И.В. *Управление защитой информации на основе интеллектуальных технологий*. М.: Машиностроение; 2013. 241 с.
5. Efimov B.I., Lozhnikov P.S. Analysis of the impact of threats to change and block responses of experts in online survey systems. *Journal of Physics: Conference Series*. *IOP Publishing*. 2020;1546(1):012079.
6. Васильев В.И., Вульфин А.М., Гузаиров М.Б. Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт. *Информационные технологии*. 2018;24(4):266–273.
7. Васильев В.И., Вульфин А.М., Гузаиров М.Б., Картак В.М., Черняховская Л.Р. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт. *Информационные технологии*. 2020;26(4):213–221.
8. Васильев В.И., Вульфин А.М., Кудрявцева Р.Т. Анализ и управление рисками информационной безопасности с использованием технологий когнитивного моделирования. *Доклады ТУСУР*. 2017;20(4):61–66.
9. Noel S., Harley E., Tam K.H., Limiero M., Share M. CyGraph: graph-based analytics and visualization for cybersecurity. *Handbook of Statistics*. *Elsevier*. 2016.35:117–167.
10. Yeboah-Ofori A. Cyber security threat modeling for supply chain organizational environments. *Future internet*. 2019;11(3):63.
11. Zografopoulos I., Ospina J., Liu X., Konstantinou C. Cyberphysical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access*. 2021;9:29775–29818.
12. Васильев В.И., Кириллова А.Д., Кухарев С.Н. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции). *Вестник УрФО. Безопасность в информационной сфере.* 2018;30(4):66–74.
13. Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт. *Информационные технологии.* 2018;24(10):657–664.
14. Васильев В.И., Кириллова А.Д., Вульфин А.М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC. *Вопросы кибербезопасности*. 2021;42(2):2–16.
15. Васильев В.И., Вульфин А.М., Кириллова А.Д. Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования. *Моделирование, оптимизация и информационные технологии*. 2022;10(2). URL: https://moitvivt.ru/ru/journal/pdf?id=1184 DOI: 10.26102/2310-6018/2022.37.2.022 (дата обращения: 13.11.2023).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Кириллова Анастасия Дмитриевна, старший преподаватель Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: kirillova.andm@gmail.com

Anastasia D. Kirillova, Senior Lecturer at Ufa University of Science and Technology, Ufa, the Russian Federation.

Вульфин Алексей Михайлович, доктор технических наук, профессор Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: vulfin.alexey@gmail.com
ORCID: 0000-0001-5857-2413

Aleksey M. Vulfin, Doctor of Technical Sciences, Professor at Ufa University of Science and Technology, Ufa, the Russian Federation.

Васильев Владимир Иванович, доктор технических наук, профессор Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: vas0015@yandex.ru

Vladimir I. Vasilyev, Doctor of Technical Sciences, Professor at Ufa University of Science and Technology, Ufa, the Russian Federation.

Гузаиров Мурат Бакеевич, доктор технических наук, профессор Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: mbguzairov@gmail.com

Murat B. Guzairov, Doctor of Technical Sciences, Professor at Ufa University of Science and Technology, Ufa, the Russian Federation.

Статья поступила в редакцию 18.11.2023; одобрена после рецензирования 01.12.2023; принята к публикации 20.12.2023.

The article was submitted 18.11.2023; approved after reviewing 01.12.2023; accepted for publication 20.12.2023.